**Krypton OverTheWire — Beginner Intern Report (Level 0 to 7)**

(Using **Kali Linux**)

## Introduction

This report explains my experience while playing the Krypton wargame on OverTheWire, using **Kali Linux**.
The goal was to practice basic cryptography (encryption and decryption) techniques.
I completed levels 0 to 7 during this exercise.

## Krypton Level 0

**Objective:**
Connect to the Krypton server and find the password for Level 1.

**Steps Taken on Kali Linux:**

- Opened **Kali Terminal**.
- Used SSH to connect:**ssh krypton0@krypton.labs.overthewire.org -p 2222**
- Entered the provided starting password.
- Listed files in the directory:**ls**
- Displayed the content of the file:**cat README**
- Copied the password for Level 1.

**Learning:**
Learned to connect to remote servers using **SSH** on Kali Linux and to navigate files with ls and cat.

## Krypton Level 1

**Objective:**
Decrypt a simple ROT13 encrypted message.

**Steps Taken:**

- Connected to Level 1 from Kali Terminal:
- ssh krypton1@krypton.labs.overthewire.org -p 2222
- Used password found from Level 0.
- Listed files:**ls**
- Opened the encrypted file:**cat krypton2**
- Decrypted using tr command:**cat krypton2 | tr 'A-Za-z' 'N-ZA-Mn-za-m'**
- Found the password for Level 2.

**Learning:**
Practiced using Kali's built-in **tr tool** for simple decryption.

## Krypton Level 2

**Objective:**
Decrypt another ROT13 encrypted message.

**Steps Taken:**

- Connected to Level 2 using SSH on Kali:**sshkrypton2@krypton.labs.overthewire.org -p 2222**
- Listed and opened files:**ls,cat krypton3**
- Applied ROT13 decryption again:**cat krypton3 | tr 'A-Za-z' 'N-ZA-Mn-za-m'**
- Retrieved the password for Level 3.

**Learning:**
Repeated usage of tr for encryption understanding on Linux.

**Krypton Level 3**

**Objective:**
Decrypt a message using a different Caesar cipher shift.

**Steps Taken:**

- Connected to Level 3: **ssh krypton3@krypton.labs.overthewire.org -p 2222**
- Listed and viewed the file: **ls,cat krypton4**
- Attempted ROT13 but output was not readable.
- Realized it's a Caesar cipher with unknown shift.
- Used Kali's browser (**Firefox ESR**) to open an online Caesar cipher decoder.
- Tried multiple shifts until correct one was found.
- Got the password for Level 4.

**Learning:**
Learned how Caesar cipher shifting differs and how to analyze if tr fails.

**Krypton Level 4**

**Objective:**
Solve a monoalphabetic substitution cipher.

**Steps Taken:**

- Connected to Level 4: **ssh krypton4@krypton.labs.overthewire.org -p 2222**
- Listed files and viewed the encrypted text:l**s,cat krypton5**
- Performed letter frequency analysis using: **cat krypton5 | grep -o . | sort | uniq -c | sort -nr**
- Identified common letters (like 'E', 'T', 'A').
- Manually replaced letters by guessing the words.
- Found the password for Level 5.

**Learning:**
Understood frequency analysis basics using Kali's Linux terminal tools like grep, sort, and uniq.

**Krypton Level 5**

**Objective:**
Decrypt a message based on a provided cipher key.

**Steps Taken:**

- Connected to Level 5: **ssh krypton5@krypton.labs.overthewire.org -p 2222**
- Listed files: **ls,cat krypton6**
- Observed a custom key mapping.
- Used sed command for simple replacements (if needed):cat krypton6 | sed 's/A/M/g; s/B/N/g; ...'
- Decoded and found the password for Level 6.

**Learning:**
Learned how custom keys can shift the whole alphabet, and how to handle it using basic Kali scripting.

**Krypton Level 6**

**Objective:**
Decrypt using a separate key file provided.

**Steps Taken:**

- Connected to Level 6: ssh krypton6@krypton.labs.overthewire.org -p 2222
- Listed files: ls,cat keyfile,cat krypton7
- Read the keyfile carefully to understand the mapping.
- Used a **Python script** on Kali or manually mapped the key to decrypt the message.
- Retrieved password for Level 7.

**Learning:**
Learned how to use external key files for decryption manually and by scripting.

**Krypton Level 7**

**Objective:**
Run an executable binary to decrypt an encrypted file.

**Steps Taken:**

- Connected to Level 7: ssh krypton7@krypton.labs.overthewire.org -p 2222
- Listed files: ls
- Made binary executable: chmod +x krypton7
- Ran the binary with the encrypted file: ./krypton7 krypton8
- The output showed the password for Level 8.

**Learning:**
Learned how to work with Linux executables in Kali, using **chmod** to give execution permission, and how to provide file inputs.

**Conclusion**

Using Kali Linux terminal and tools helped me understand:

- Secure connection with SSH.
- Basic file handling (ls, cat).
- ROT13, Caesar cipher, and substitution cipher solving.
- Frequency analysis using terminal commands.
- Writing small scripts for mapping and decoding.